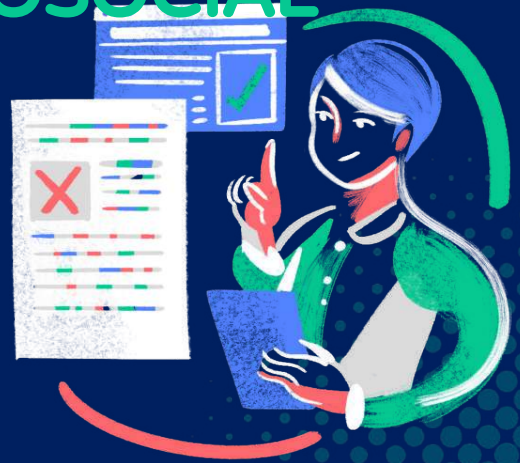
LARPSICO

BALANCE DE SITUACIÓN Y PERSPECTIVAS DE LA CIBERSEGURIDAD LABORAL EN CLAVE DE PREVENCIÓN PSICOSOCIAL

María Marta Martínez Jiménez

Francisco Manuel Extremera Méndez



Start Now

Aumento del riesgo de sufrir ciberataques: nuevas obligaciones y desafíos para las empresas más allá de la brecha de información.

Ante una sociedad cada vez más hiperconectada, no es de extrañar que **aumente el número de ataques cibernéticos**, en 2023 **este incremento supuso un 14% con respecto al año anterior** y fueron identificadas casi **29.000 ataques.**

Ante este escenario, **únicamente un 4% de las empresas tienen correctamente protegidos** tanto a sus personas trabajadoras como a sus sistemas de recibir un posible ataque cibernético. **6 de cada 10 empresas se han visto expuestas a algún tipo de ataque de estas características.**

Pero, esto no ocurre sólo en organizaciones, sino que puede llegar a afectar a **cualquier persona y en cualquier lugar,** por lo que, debemos entender que **ha de caracterizarse como un "riesgo social global"**

La Unión Europea vuelve a dar un paso adelante en materia de ciberseguridad: Directiva NIS II.

Ante este escenario, la UE actúa volviendo a dar un paso muy relevante normativamente con la finalidad de **adaptar las leyes a la evolución de la realidad tecnológica, muy cambiante y acelerada.**

De este modo, tras la adopción de **la Directiva NIS I en 2016,** vuelve a adoptar una norma en materia de ciberseguridad, **la Directiva 2022/2556 o NIS II** al objeto de garantizar un nivel elevado y homogéneo de seguridad en todo el mercado único digital europeo.

Nuevas obligaciones que han de cumplir las empresas europeas con especial referencia para aquellas que tienen más de 50 personas trabajadoras y para los sectores considerados críticos, con el objetivo de **mejorar la capacidad de hacer frente a las redes digitales y los sistemas informáticos.**

Hace mención a la **importancia de la formación en ciberseguridad a las personas empleadas**, por lo que, el cumplimiento efectivo de los deberes pesa sobre la plantilla.

Las medidas sobre ciberseguridad llegan al terreno laboral a través de la *"ciberseguridad en el trabajo"*.

La ciberseguridad se postula como uno de los **aspectos de mayor relevancia estratégica para las empresas**, convirtiéndose en pilar imprescindible para su crecimiento y estabilidad.

Como se ha indicado desde el **LARPSICO**, la ciberseguridad también despliega sus efectos en el terreno laboral. **Esta dimensión laboral de la política de seguridad cuenta con un sector especializado denominado *"ciberseguridad en el trabajo"*.**

> Con este concepto, hacemos referencia al **conjunto de las medidas técnicas y organizativas adoptadas por las empresas como política de protección de la seguridad informativa.**

Según el **INCIBE**, gracias a tales medidas, las empresas logran implantar una política de seguridad interna de la organización que **permite transmitir a los empleados obligaciones y buenas prácticas en relación con la seguridad de la información.**

¿Tienen las empresas el deber legal de actuar en materia de ciberseguridad laboral?

A nivel Europeo, la Directiva NIS II amplía las medidas que deben adoptarse: Implantar un sistema de autenticación multifactor (MFA); controlar el acceso a los sistemas y aplicaciones con un nivel mínimo de permisos; asegurar cadena de suministro; implantar sistemas de prevención frente a ciberataques y sistemas de continuidad de negocio.

A nivel nacional, el Real Decreto-ley 12/2018 de seguridad de las redes y sistemas de información:

Su artículo 16 impone la obligación de *"**adoptar medidas técnicas y de organización, adecuadas y proporcionadas, para gestionar los riesgos que se planteen para la seguridad de las redes y sistemas de información**"*.

En cualquier caso, La obligación de las empresas de actuar en materia de ciberseguridad en el entorno laboral se desprende igualmente de la r**egulación materia de protección de datos**, aplicable al conjunto de las empresas.

El artículo 32 del RGPD y el artículo 9.1. de la LOPD, eque señala que la empresa responsable del tratamiento estará obligada a aplicar *"**medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo…**"*.

Adopción de medidas en materia de ciberseguridad, una obligación de medios según los tribunales.

La doctrina judicial ha señalado que **un ataque cibernético puede tenerse como un riesgo imprevisible o inevitable, esto es, una situación de fuerza mayor** (SAN 37/2022, 14 de marzo, cuyo fallo ha sido confirmado por la STS, 4ª, 908/2024, de 11 junio de 2024).

Por este motivo, **la diligencia empresarial de ciberseguridad no se trata de obligación de resultado, sino de medios,** es decir, basta con poner los medios adecuados, para evitar los daños derivados de los ciberataques informáticos (STS, 3ª, 188/2022, 15 de febrero).

Corresponde a la empresa la prueba de haber desplegado ese deber de conducta diligente, pues en otro caso el riesgo actualizado en daño le será imputable. La empresa puede certificar que ha actuado diligentemente

La Organización Internacional de Normalización (ISO), ha desarrollado la ISO 27001, que pretende asegurar la confidencialidad, integridad y disponibilidad de la información de una organización y de los sistemas y aplicaciones que la tratan.

La formación de las personas trabajadoras: clave de bóveda de la ciberseguridad laboral.

Dentro de tales medidas **adquiere especial relevancia la formación de las personas trabajadoras en materia de ciberseguridad.** Desde el LARPSICO se ha señalado que la **clave de bóveda de las políticas de ciberseguridad en las empresas** está en la concienciación, y capacitación, a las personas empleadas.

Cada una de las personas empleadas **deben afrontar competencias de ciberseguridad para que sus puestos de trabajo sean entornos ciberseguros**, no solo las personas profesionales que deben vigilar para prevenir que tengan éxito los ciberataques y las fugas de seguridad.

La realidad demuestra que **los ciberataques y las filtraciones de datos suelen ocurrir debido al desconocimiento** de las prácticas adecuadas de seguridad informática **por parte de las personas empleadas.**

El 90% de todos los ciberataques están causados por errores humanos, considerándose éste el principal motivo por el que se producen las brechas de información en la empresa.

Implementación de medidas de ciberseguridad laboral: nuevas obligaciones para las personas trabajadoras.

Consecuencia de esta mayor formación y concienciación de las personas trabajadoras en materia de seguridad, **se implementan para ellas nuevas obligaciones que deben ser tenidas en cuenta por cada una de ellas.**

El INCIBE recoge entre algunas de las obligaciones más importantes de las personas trabajadoras las siguientes: obligación de mantener la confidencialidad en relación con cualquier información a la que tenga acceso; de notificar cualquier incidente de seguridad relacionado con el puesto de trabajo.

Sin duda una mayor carga para las personas trabajadoras que, junto con el miedo que en muchas de peleas genera el riesgo de sufrir un ciberataque **presenta importantes consecuencias en el terreno de la prevención de riesgos psicosociales.**

La ciberseguridad: una cuestión importante para todas las empresas, también para las PYMES.

Los ciberataques **representan una amenaza constante para todas las empresas, independientemente de su sector o tamaño**, a pesar de que tienen mayor presencia en sectores estratégicos como el financiero .

Los protocolos de seguridad y **la ciberseguridad para PYMES deben ser una prioridad para quienes buscan proteger su negocio.** En este sentido, el informe de Kaspersky de 2022, señala que casi **2 de cada 3 PYMES de todo el planeta han sufrido un ataque cibernético.**

Google ha señalado que el **49% de las pequeñas y medianas empresas han tenido algún problema de ciberseguridad**; , cuando se habla de r**obo de información o pérdida de datos, se eleva al 70%.**

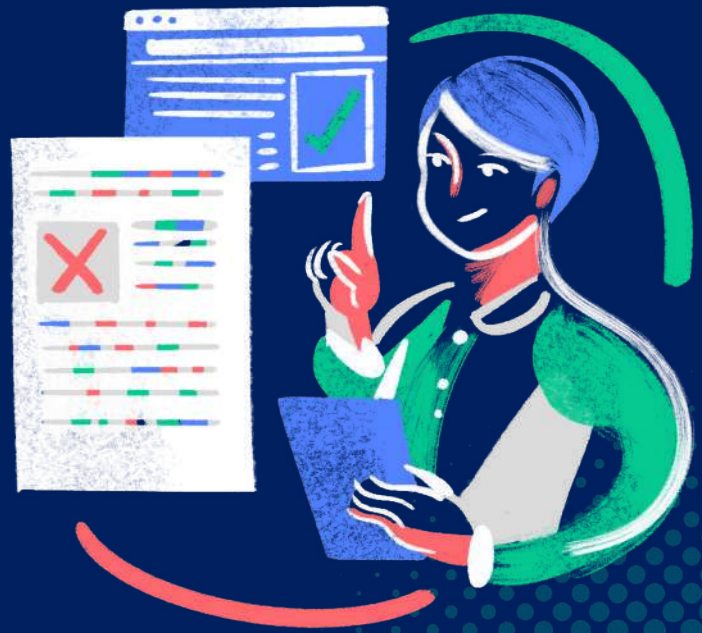
Desde el LARPSICO se ha señalado la **importancia de que las PYMES cuenten con medios de apoyo por parte de las AAPP** pues éstas, aunque no cuentan con los mismos medios que las grandes, sí que están expuestas a amenazas cibernéticas análogas: **Plan España Digital.**

LARPSICO

RIESGOS PSICOSOCIALES

LA OTRA CARA DE LA MONEDA DE LA CIBERSEGURIDAD

Start Now



LARPSICO

¿LA CIBERDELINCUENCIA SOLO AFECTA A LAS EMPRESAS?

La actualidad, nacional e internacional, viene marcada claramente por esta nueva tipología de riesgos tecnológicos y sociales. Las personas, así como, las empresas e instituciones se encuentran cada vez más expuestas a los ataques, como ha ocurrido recientemente al cuerpo de la Guardia Civil al quedar expuestos sus datos médicos a través de un ataque mediante el ransomware "lockbit" 3.0

LARPSICO

TIPOS DE CIBERAMENAZAS

Malware

Es un programa informático (software, en inglés) cuya principal característica es la ejecución sin el conocimiento ni autorización del propietario o usuario del equipo infectado y realiza funciones en el sistema que son perjudiciales para el usuario y/o para el sistema.

Ransomware

Es un tipo de malware que toma por completo el control del equipo bloqueando o cifrando la información del usuario para, a continuación, pedir dinero a cambio de liberar o descifrar los ficheros del dispositivo

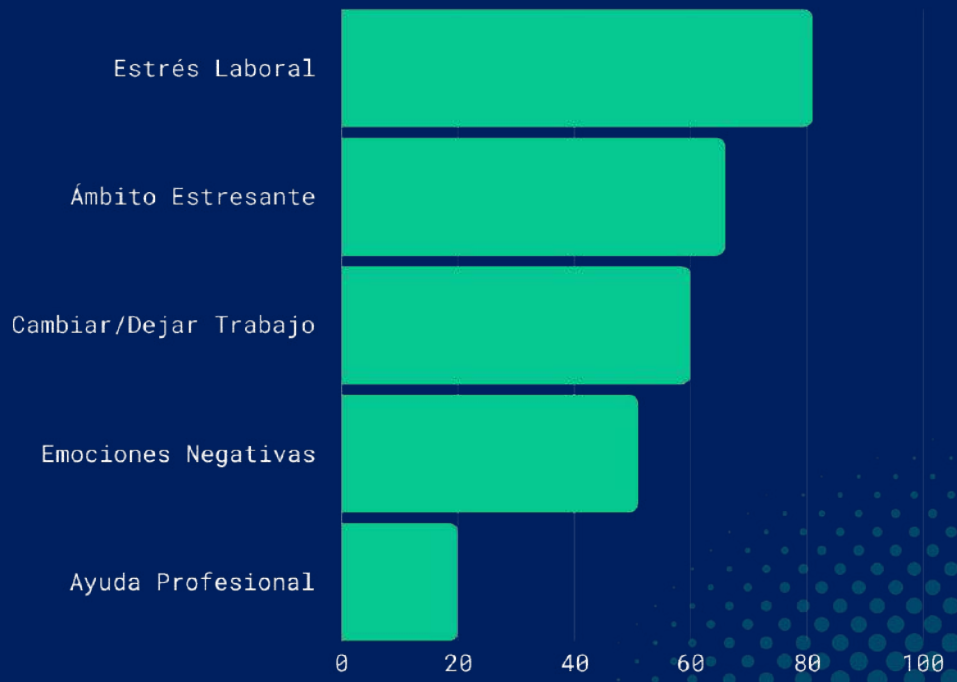
Fuente: INCIBE

LARPSICO

DATOS PREOCUPANTES

ISACA: 66% de los profesionales de la ciberseguridad dice ser de este ámbito que es más estresante que hace cinco años, el 81% reconoce que ha aumentado el estrés ante un cuadro sucesivo de amenazas y más del 60% han considerado cambiar o dejar el puesto de trabajo debido al estrés que este le puede llegar a generar.

LARPSICO: (51%) de los profesionales dicen experimentar emociones negativas (ira, ansiedad, depresión) al sentirse desbordados por el trabajo; dos de cada cinco (20%) han tenido que buscar ayuda profesional debido al impacto físico del estrés laboral (migrañas, ataques de pánico o presión arterial alta).



LARPSICO

ESPECIAL TRANCENDENCIA SOCIOLABORAL

SAN 37/22, 14 marzo

La empresa presenta un ERTE-FM al recibir un ataque informático viéndose obligados a paralizar la actividad. Se entiende que la empresa ha actuado con la debida diligencia en términos de ciberseguridad.

STS 908/2024,11 junio

Ratifica la postura adoptada previamente por la Audiencia Nacional

STSJ Cataluña 13/2024, 12 enero

Reconoce una incapacidad temporal por estrés laboral ocasionado por la visión de vídeos de contenido extremo para evitar que estos no llegasen a las redes sociales propiedad de la empresa que recibe la condena.

LARPSICO

¿QUÉ FOMENTA EL ESTRÉS LABORAL?

Aumento de la demanda y carga de trabajo:

Las amenazas cibernéticas se vuelven cada vez más sofisticadas, los recursos limitados y la escasez de personal laboral para hacer frente a las tareas de protección frente a este tipo de ataques.

Insuficiencia de control y apoyo:

Escasez de personal con las habilidades necesarias, los recursos limitados, la incomprensión de las empresas que genera una clara falta de apoyo hacia las personas trabajadoras.

Falta de información y de participación:

Falta de formación de las personas trabajadoras en competencias digitales, así como de consulta o participación por su parte a la hora de introducir cambios tecnológicos en las empresas.

LARPSICO

ESTUDIO DE CASOS CONCRETOS

UNIQLO, España

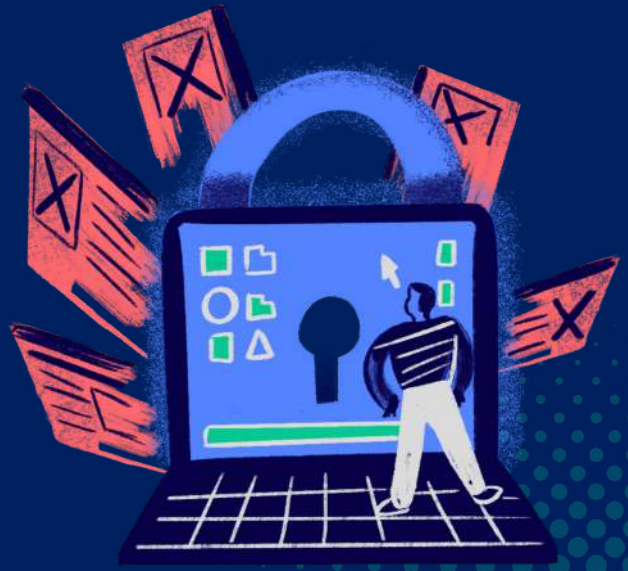
450.000 euros de multa a una empresa porque un miembro de recursos humanos, por error, mandó a un trabajador las nóminas de 446 personas empleadas.

La empresa incurre en una infracción grave al no garantizar la seguridad de los datos, lo que permitió que un error humano divulgara la información confidencial a una persona no autorizada.

COMMCENTER, SA

STS, 3ª, 188/2022. Se confirma la sanción de 40.000 euros a la empresa por falta de adopción de medidas técnicas necesarias para garantizar la seguridad de los mismos.

La empresa responsable del tratamiento estará obligada a aplicar esas medidas o un mecanismo de certificación (art. 42 RGPD).



LARPSICO

¿QUÉ PAPEL TIENE LA NEGOCIACIÓN COLECTIVA?

CC Mercadona

Se reserva el derecho de "verificar" con programas informáticos "la correcta utilización de los medios y dispositivos electrónicos propiedad de la empresa"

CC Banca y CC Iberdrola

Formación de las competencias digitales, pero además, comprende un capítulo amplio sobre ciberseguridad y el uso de herramientas tecnológicas

C. Colaboración INCIBE

Formaciones en el ámbito de la ciberseguridad destinadas a aquellas personas de colectivos más vulnerables o infrarrepresentados que puedan integrarse de la forma más adecuada.

LARPSICO

MUESTRAS ADICCIONALES

XXV CC Nokia Spain, SA

Art. 42: Teletrabajo

Protección de datos y seguridad de la información. Se establecerá que el protocolo de acceso a los medios, intranet, correo electrónico de la Empresa et. será el fijado por esta última, que incluirá una identificación única de la persona trabajadora, y un medio de acceso remoto y validación vía VirtualPrivateNetwork con doble mecanismo de identificación, a través de otra clave enviada a través de

CC Grupo Allianz

Art. 41: Utilización de Herramientas telemáticas

Las Secciones Sindicales de Grupo serán responsables del contenido de sus envíos, del buen uso de ambos instrumentos, y normas generales en materia de utilización de correo electrónico. Asimismo, de los ficheros que las empresas pudieran haberles puesto a su disposición, asumiendo enteramente la responsabilidad a efectos de la LOPDD.

CC Hermandad Farmaceútica del Mediterráneao, SCL

Art.7: Normativa de uso de los sistemas de información

Sistema de Gestión de la Seguridad de la Información (SGSI) como medio eficaz de minimizar los riesgos tecnológicos. Para ello ha adoptado controles y procedimientos de seguridad más eficaces y coherentes con la estrategia de negocio. Como parte de las medidas a implantar ha elaborado una nueva «Normativa de uso de los sistemas de información de Hefame»

LARPSICO

BUENAS PR ÁCTICAS

OX SECURITY

Supervisa 129 aplicaciones y clasifica más de 119.000 alertas de seguridad al año. En lugar de «luchar contra la marea», han considerado un cambio de perspectiva.

ESTRATEGIAS IMPLEMENTADAS:

- Evalución de Riesgos Psicosociales
- Formación Continua
- Apoyo psicológico y de la Dirección
- Flexibilidad en el Trabajo

CASO DE ÉXITO CLÍNICA - INCIBE

Ej.https://www.incibe.es/empresas/que-te-interesa/proteccion-puesto-trabajo

El acceso al teletrabajo: una puerta abierta para los ciberdelincuentes.

Según la suma de los datos del INCIBE y el Ministerio de Defensa, **el teletrabajo ha incrementado la exposición y ha provocado un aumento de ciberataques.**

El aumento en la frecuencia de ciberataques relacionados con el teletrabajo ha sido significativo: **en algunos casos se han incrementado en hasta un 300% debido a las vulnerabilidades adicionales de esta modalidad de trabajo.**

Este riesgo elevado de sufrir ciberataques incrementa la sensación de vulnerabilidad de las personas que optan por el teletrabajo, lo que **deriva en la exposición a factores de riesgos psicosociales como el estrés o la ansiedad laboral.**

El INCIBE ha desarrollado una Guía sobre ciberseguridad en teletrabajo. Esencial hacia teletrabajo seguro es el establecimiento de una **política organizativa sobre teletrabajo.**

Incide en **cuatro aspectos que considera esenciales:** asegurar los equipos de trabajo; asegurar los dispositivos móviles de teletrabajo; proteger los datos en terminales de teletrabajo; hacer copias de seguridad de los datos en dispositivos teletrabajo.

Conclusiones: Hacia la supresión del malestar psicosocial asociado a la ciberseguridad: perspectivas cooperación y enfoque integral de la cuestión.

A. En el ámbito de la ciberseguridad laboral, **el foco debe situarse en el factor humano**, el cual representa una parte igualmente importante del problema de la ciberseguridad.

> **No puede obviarse por tanto la gestión preventiva en materia de ciberseguridad**, siendo fundamental que esta nueva responsabilidad laboral sea tenida en cuenta en el sistema de **gestión preventiva de riesgos psicosociales de las empresas.**

B. Para ello, tal y como ha indicado la AESST, es **necesario que la ciberseguridad laboral y la prevención de riesgos laborales, se enfrenten por las empresas desde un enfoque conjunto**, es decir, no pueden considerarse actividades independientes, sino que deben llevarse a cabo conjuntamente.

C. A tal fin, como se señala desde el LARPSICO, **la cooperación entre las funciones de seguridad informática y los sistemas de seguridad y salud en el trabajo** será necesaria para que esta protección no se haga sobre el malestar psicosocial de las personas empleadas

D. Un mayor enfoque en el bienestar de las personas empleadas en ciberseguridad, una mejor formación y las herramientas adecuadas cambiarán la situación de creciente malestar psicosocial asociado a la carga de ciberseguridad de las personas trabajadoras.

LARPSICO

LARPSICO

MUCHAS

GRACIAS

THE END